BRYAN SCHRODER
Acting United States Attorney

RICHARD L. POMEROY
YVONNE LAMOUREUX
ADAM ALEXANDER
Assistant U.S. Attorneys
Federal Building & U.S. Courthouse
222 West Seventh Avenue, #9, Rm. 253
Anchorage, Alaska 99513-7567
Telephone: (907) 271-5071
Facsimile: (907) 271-2344
Richard.Pomeroy@usdoj.gov
Yvonne.Lamoureux@usdoj.gov
Adam.Alexander@usdoj.gov

ETHAN ARENSON
HAROLD CHUN
FRANK LIN
Trial Attorneys
Computer Crime & Intellectual Property Section
1301 New York Avenue, NW, Suite 600
Washington, DC 20005
Telephone: (202) 514-1026
Facsimile: (202) 514-6113
Ethan.Arenson@usdoj.gov
Harold.Chun@usdoj.gov
Frank.Lin@usdoj.gov

Attorneys for Plaintiff United States

//

//

//

//

//

//

//

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	Case No. 3:17-cv-00____
	)	
v.	)	**FILED *EX PARTE***
	)	**AND UNDER SEAL**
PETER YURYEVICH LEVASHOV,	)	
a/k/a "Petr Levashov," "Peter Severa,"	)	
"Petr Severa," and "Sergey Astakhov",	)	
	)	
Defendant.	)	

COMPLAINT

Plaintiff, the United States of America, by and through its undersigned counsel, alleges the following:

1. This is a civil action brought under Title 18, United States Code, Sections 1345 and 2521, and Federal Rule of Civil Procedure 65, to enjoin the Defendant from continuing to engage in wire fraud and unauthorized interception of electronic communications in violation of Title 18, United States Code, Sections 1343 and 2511, by means of malicious computer software ("malware") known as Kelihos.

2. Kelihos is malware that enlists infected computers into a "botnet" – a network of other compromised computers controlled by the Defendant. Individual infected computers, or "bots," are controlled remotely through a decentralized command and control ("C&C") system in which infected computers, or "peers," remain in contact with each other.

3. Once infected by Kelihos, compromised computers within the botnet are used by the Defendant to generate huge volumes of unsolicited "spam" emails that advertise counterfeit drugs, pump-and-dump stock schemes, work-at-home scams, and other frauds. Kelihos is also used to generate phishing emails, harvest user credentials, and to download additional malware onto victim computers, including ransomware and banking Trojans.

Parties

4. Plaintiff is the United States of America.

5. Defendant Peter Yuryevich Levashov is citizen of Russia who resides in St. Petersburg. Defendant uses the aliases Petr Levashov, Peter Severa, Petr Severa, and Sergey Astakhov.

Jurisdiction and Venue

6. Subject matter jurisdiction lies pursuant to Title 18, United States Code, Sections 1345(a)(1) and 2521 and Title 28, United States Code, Sections 1331 and 1345.

7. Defendant is subject to the personal jurisdiction of this Court, having infected computers, used infected computers in furtherance of his scheme to defraud, and engaged in unauthorized wiretapping, all within the District of Alaska. The Defendant has also sent numerous fraudulent and malicious electronic messages to persons within the District of Alaska.

8. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2).

//

The Defendant's Scheme to Defraud and Engage in Illegal Interception

9. The Defendant is one of the world's most notorious criminal spammers who was first indicted in the Eastern District of Michigan for email and wire fraud more than a decade ago. The charges arose out of the Defendant's use of illegal spam to promote pump-and-dump penny stock schemes.

10. In 2009, the Defendant was again the subject of criminal charges, this time in the District of Columbia. The D.C. criminal complaint charges the Defendant with computer fraud violations arising from his operation of the "Storm" botnet, a predecessor to Kelihos that was also used to distribute illegal spam.

11. The Defendant has long been a fixture on the list of the World's Ten Worst Spammers, which is maintained by the anti-spam organization Spamhaus. Currently, the Defendant occupies the sixth spot on the list.

The Defendant's Use of Kelihos

12. Since about 2010, the Defendant has been the operator of the Kelihos botnet, a network of computers infected with malware distributed by the Defendant.

13. Kelihos is a sophisticated malware variant that is used by the Defendant to harvest user credentials from victim computers, propagate huge quantities of spam emails, and to distribute other forms of malware.

14. The Kelihos malware harvests user credentials from victim computers through a number of methods. First, Kelihos searches text-based files stored on victim computers for email addresses. Second, Kelihos searches locations on victim computers for files known to contain usernames and passwords, including files

associated with Internet browsers Chrome, Firefox, and Internet Explorer. Any email addresses and passwords located in these searches are harvested by Kelihos and subsequently transmitted back to the Defendant.

15. To capture additional user credentials, Kelihos installs a software program called WinPCAP on infected machines. WinPCAP is a powerful packet capture utility that intercepts, in real time, electronic communications traversing the victim computer's network card. Usernames and passwords found within this network traffic are transmitted back to the Defendant.

16. The credential harvesting operation described above is used by the Defendant to further his illegal spamming operation. The Defendant promotes his spamming operation by placing advertisements in various online criminal forums in which the Defendant promotes his ability to deliver spam email. In his ads, the Defendant states that he launches spam from "several thousand clean IP addresses and accounts," a technique that increases the chances that the Defendant's spam emails will evade the filters put in place by email providers seeking to protect their customers.

17. The "clean" IP addresses and accounts that power the Defendant's spamming operation are, in fact, the coopted IP addresses and/or email accounts of Kelihos victims. These IP addresses and email accounts are leveraged by the Defendant in two ways. In some cases, the Defendant instructs the bots in his Kelihos botnet to send spam directly, in essence turning victim computers into mail servers that distribute spam to the recipient email addresses provided by the

Defendant. In other cases, the Defendant leverages the credentials harvested by Kelihos to gain unauthorized access to commercial email servers, which are then used to transmit the spam messages. In these instances, the spam messages sent by the Defendant appear to originate directly from the victim's email account.

18. The spam campaigns initiated by the Defendant vary in content based on customer demand, and the Defendant differentiates his pricing based on the nature of the spam messages. In his forum advertisements, the Defendant offers to deliver one million spam messages promoting "legal" products such as "adult, mortgage, leads, pills, replics [*i.e.*, counterfeit goods], etc." for $200. The Defendant's price increases to $300 per million messages for "job spam," messages seeking to recruit job seekers into fraudulent positions, including "mules" – persons recruited to launder money and goods stolen by criminals. The Defendant also professes his willingness to propagate "scam/phishing attacks," which the Defendant promises to deliver for $500 per million messages.

19. In conversations possessed by the FBI, the Defendant provided additional insight into his pricing structure. In these conversations, the Defendant offers to send messages that would infect users with a type of malware known as ransomware – malicious software that encrypts the contents of victim computers and then demands a ransom to return the encrypted files to a readable state. The Defendant's price: $500 per million emails. In the same conversation, the Defendant offers to send emails promoting a pump-and-dump penny stock scheme, designed to drive up the price of a thinly-traded security. For these messages, the

Defendant demanded a commission based on the movement in the stock's price that occurred as a result of the spam campaign.

20. In addition to using Kelihos to distribute spam, the Defendant also profits by using Kelihos to directly install malware on victim computers. During FBI testing, Kelihos was observed installing ransomware onto a test machine, as well as "Vawtrak" banking Trojan (used to steal login credentials used at financial institutions), and a malicious Word document designed to infect the computer with the Kronos banking Trojan.

21. The Defendant and those acting at his direction have infected hundreds of thousands of computers around the world with Kelihos, including computers within the District of Alaska.

22. Persons in this District have also been the target of fraudulent and malicious spam emails that the Defendant has sent via the Kelihos botnet. These targets include employees of Alaska's public school districts, thousands of customers of Alaskan internet service provider General Communication Inc. (GCI), employees of the cities of Anchorage and Juneau, and employees of the Alaska Division of Occupational Licensing.

COUNT I
(Injunctive Relief under 18 U.S.C. § 1345)

23. The United States of America alleges and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

24. The Defendant is engaged in wire fraud, in violation of Title 18, United States Code, Section 1343, in that the Defendant, having devised a scheme or

artifice to defraud and for obtaining money by means of false or fraudulent pretenses, is transmitting and causing to be transmitted, by means of wire communication in interstate and foreign commerce, writings, signs, and signals for the purpose of executing such scheme or artifice.

25. Pursuant to Title 18, United States Code, Section 1345(a) and (b), the United States of America requests the issuance of a temporary restraining order, preliminary injunction, and permanent injunction against the Defendant and his agents in order to prevent a continuing and substantial injury to the owners and legitimate users of the infected computers in the Kelihos botnet.

COUNT II
(Injunctive Relief under 18 U.S.C. § 2521)

26. The United States of America alleges and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

27. The Defendant is engaged in the unauthorized interception of electronic communications, in violation of Title 18, United States Code, Section 2511, in that the Defendant is intentionally intercepting electronic communications, and is intentionally using and endeavoring to use the contents of electronic communications knowing that the information is obtained through the unauthorized interception of electronic communications.

28. Pursuant to Title 18, United States Code, Section 2521, the United States of America requests the issuance of a temporary restraining order, preliminary injunction, and permanent injunction against the Defendant and his

agents in order to prevent a continuing and substantial injury to the owners and legitimate users of the infected computers in the Kelihos botnet.

PRAYER FOR RELIEF

WHEREFORE, the United States of America prays that the Court:

A. Enter judgment in favor of the Government and against the Defendant;

B. Pursuant to Title 18, United States Code, Sections 1345(b) and 2521, enter a preliminary injunction and permanent injunction against the Defendant and his agents, servants, employees, and all persons and entities in active concert or participation with them from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity from engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein;

C. Pursuant to Title 18, United States Code, Sections 1345(b) and 2521, enter a preliminary injunction and permanent injunction authorizing the Government to continue the malware disruption plan specified in the Government's Memorandum of Law in Support of Motion for Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction, for a period of six months, and requiring the entities specified in the Temporary Restraining Order to continue to take the actions specified in the Temporary Restraining Order for a period of six months;

D. Order such other relief that the Court deems just and proper.

Dated: April 4, 2017

BRYAN SCHRODER
Acting United States Attorney

By: /s/ Richard Pomeroy
RICHARD POMEROY
YVONNE LAMOUREUX
ADAM ALEXANDER
Assistant U.S. Attorneys
District of Alaska

KENNETH A. BLANCO
Acting Assistant Attorney General

By: /s/ Ethan Arenson
ETHAN ARENSON
HAROLD CHUN
FRANK LIN
Trial Attorneys
Computer Crime and
Intellectual Property Section